Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
24 May 2018	1.0	Vivekkumar Mehta	First version of functional safety concept

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept will help in identifying new requirements and allocate these requirements to system diagrams. The functional safety concept is looking at the item from a higher level. The functional safety concept looks at the general functionality of the item.

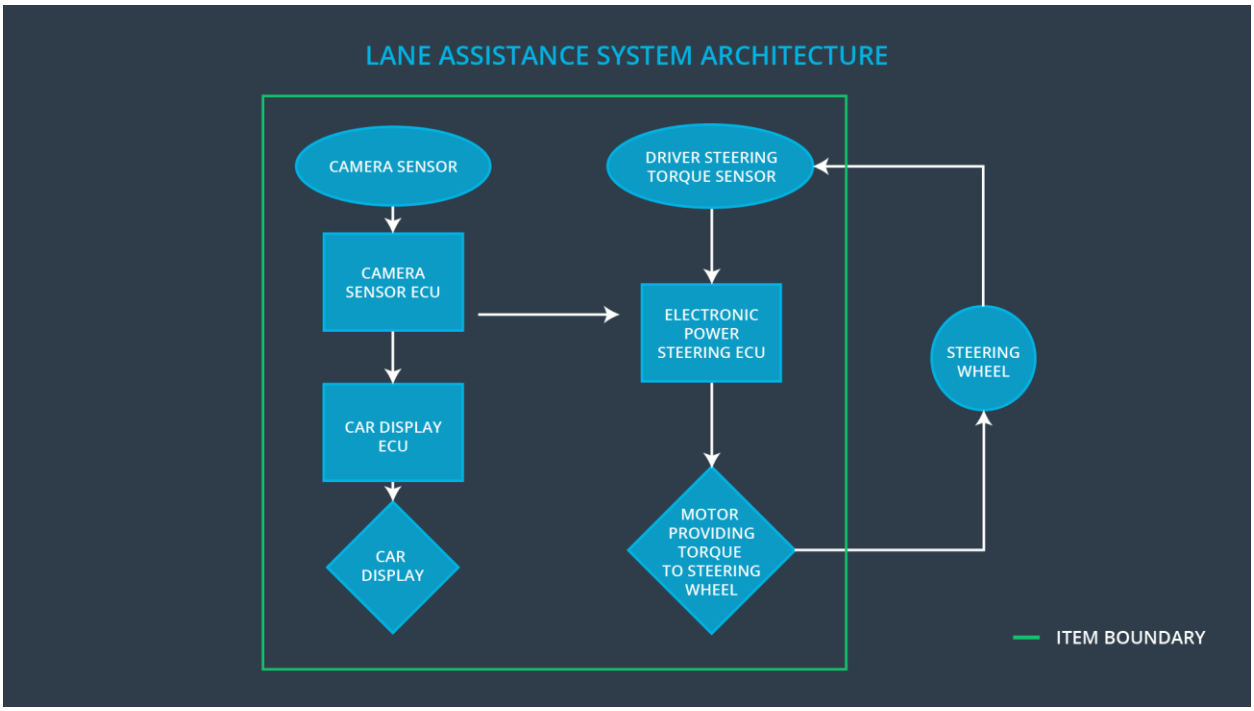
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The LDW steering torque function shall be limited.
Safety_Goal_02	LKA function excess usage shall be alerted or stopped after certain time limit

Preliminary Architecture

This figure describes architecture of Lance assistance system.



Description of architecture elements

Element	Description
Camera Sensor	Provides visual input to camera sensor ECU
Camera Sensor ECU	Detects ego lane lines and gives torque input to Electronic power steering ECU.

Car Display	Gives visual feedback to driver
Car Display ECU	Generates warning signals from camera sensor ECU and electronic power steering ECU
Driver Steering Torque Sensor	Gives steering torque input to electronic power steering ECU given by driver
Electronic Power Steering ECU	Gets steering input from driver and camera sensor ECU, computes final torque and gives it to steering wheel motor.
Motor	Receives final torque and applies it to steering wheel.

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The LDW function applies too much torque with high amplitude (above limit).
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The LDW function applies too much torque with high oscillations (above limit).

Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The LKA functions works randomly when camera sensor is not working.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque *amplitude* is below Max_Torque_Amplitude	C	50 ms	Lane Assistant functionality off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque *frequency* is below Max_Torque_Frequency	C	50 ms	Lane Assistant functionality off

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	Test how drivers react to different torque amplitudes to prove that an appropriate value was chosen.	Verify that system turns off if LKA ever exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that an appropriate value was chosen.	Verify that system turns off if LKA ever exceeds Max_Torque_Frequency.

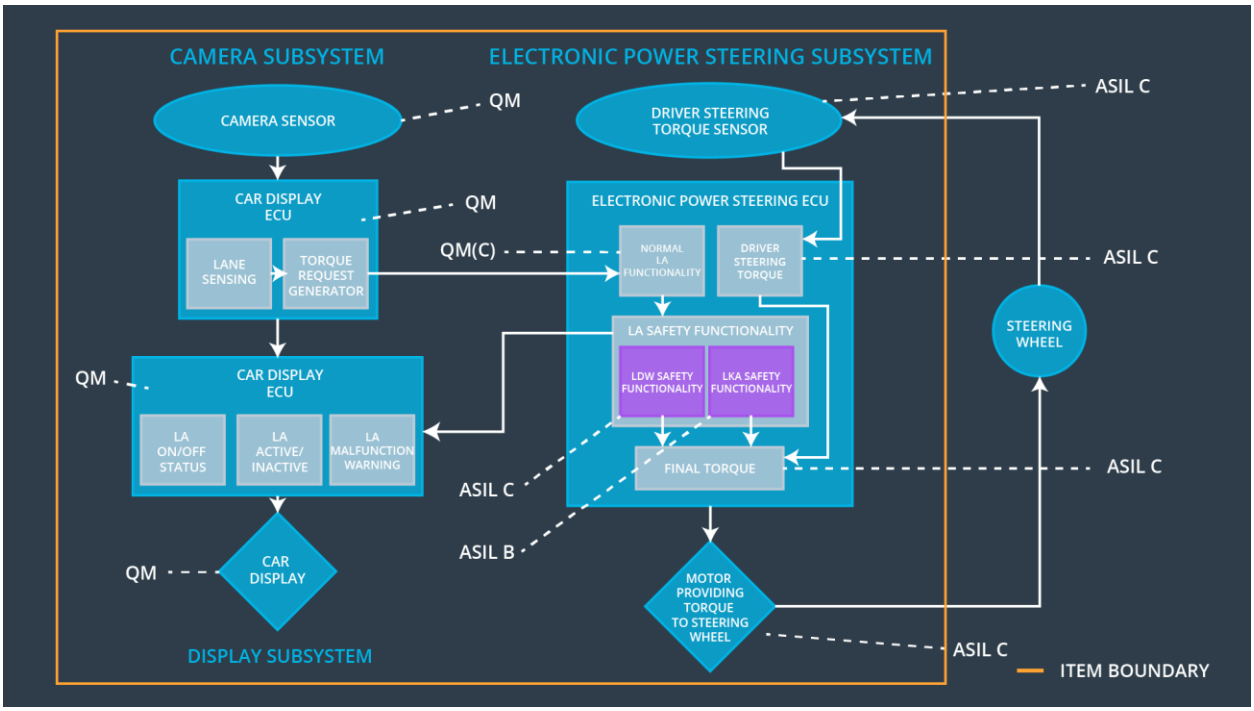
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Lane Assistant functionality off
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane_Not_Found is true	A	50 ms	Lane Assistant functionality off
Functional Safety Requirement 02-03	The camera sensor ECU shall not request torque if Laneline_Is_Yellow is stated true by camera sensor ECU.	D	25 ms	Lane Assistant functionality off

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Test and validate that the Max_Duration chosen really dissuades drivers from taking their hands off the wheel.	Verify that system turns off if LKA ever exceeds MAX_DURATION.
Functional Safety Requirement 02-02	Test and validate that Lane_Not_Found is stated correctly if lane lines cannot be detected.	Verify that system turns off if Lane_Not_Found is true.
Functional Safety Requirement 02-03	Test and validate that Laneline_Is_Yellow is stated correctly, if lanelines turn yellow.	Verify that system turns off if Laneline_Is_Yellow is true.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque *amplitude* is below Max_Torque_Amplitude	**x**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque *frequency* is below Max_Torque_Frequency	**x**		
Functional Safety	The electronic power steering ECU shall ensure that the lane	**x**		

Requirement 02-01	keeping assistance torque is applied for only Max_Duration.			
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane_Not_Found is true	**x**		
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Laneline_Is_Yellow is true	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Assistant functionality	Malfunction_01	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-02	Turn off Lane Assistant functionality	Malfunction_02	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-03	Turn off Lane Assistant functionality	Malfunction_03	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-04	Turn off Lane Assistant functionality	Malfunction_04	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-05	Turn off Lane Assistant functionality	Malfunction_05	Yes	Lane Assistant Malfunction Warning on Car Display